Amendments to the Drawings:

Figure 5 is amended by replacing the plus symbol (" + ") with the exclusive-or symbol (" $\oplus$ ") as indicated in the Office Action dated March 29, 2007.

Attachment: Replacement Sheet
Annotated Sheet Showing Changes

REMARKS/ARGUMENTS

Claims 1, 9, and 17 are pending in the present application. Applicants have amended claims 1, 9, and 17 and cancelled claims 2-8, 10-16, and 18-24 from further consideration in this application. Applicants are not conceding in this application that those claims are not patentable over the art cited by the Examiner, as the present claim amendments and cancellations are only for facilitating expeditious issuance of the application. Applicants respectfully reserve the right to pursue these and other claims in one or more continuations and/or divisional patent applications. By this response, independent claims 1, 9, and 17 are amended to include the content of claims 2-8, 10-16, and 18-24, respectively. In addition, claims 1, 9, and 17 are amended to clarify the server-generated random value from the client-generated random value and to clarify the claims in general. Support for the amendment to the claims is located at least on page 11, line 1, through page 16, line 12; and in Figures 4, 5, 6, 7A and 7B. Reconsideration of the claims is respectfully requested.

I. Telephone Interview

Applicants thank Examiners Harris Wang and Tajhi Arani for the courtesies extended to Applicants' representatives during the June 13, 2007 telephone interview. During the interview, Applicants' representatives discussed the distinctions between proposed claim amendments and the cited references. Additionally, Applicants pointed out that Mohammad Peyravian is a common inventor for both the cited *Peyravian* IBM reference and the presently claimed IBM patent application. No agreements were reached. The substance of the telephone interview is included in the following remarks.

II. 35 U.S.C. § 103, Obviousness

The Examiner has rejected claims 1-3, 6-11, 14-19 and 22-24 under 35 U.S.C. § 103 as being unpatentable over *Peyravian et al.*, "Method for Protecting Password Transmission", Computers and Security, Vol. 9, No. 5, pp.466-469, 2000, hereinafter referred to as *Peyravian*, in view of *ATIS committee*, www.atis.org, definition of Message Authentication Code, hereinafter referred to as *ATIS*. This rejection is respectfully traversed.

As to claims 1-3, 6-11, 14-19 and 22-24, the Office Action states:

> Regarding Claim 1,
>
> Peyvarian teaches the computer network, comprising: a client and a server connected by a network connection,
>
> wherein the client has a userid and a password associated with the client *("The user submits his userid (id) and password (pw) to the client" pg. 4)*;
>
> wherein the client requests access to the server by sending a first set of values to

the server *("The client generates a random value (rc) and sends id and rc to the server" pg. 4)*;

wherein the server responds to the client by generating a first random value and sending the token to the client; *("The server generates a random value (rs) and sends it to the client" pg. 4). The Examiner interprets the nonce (rs) as the token.*

wherein the client retrieves the first random value from the challenge token and sends the first random value and the userid to the server; *("the client sends id and auth_token to the receiver pg. 4, the auth_token is comprised of a hash of inputs idpw_digest, rc, and rs, the Examiner interprets rs as both the random value and token")*

wherein the server verifies the received first random value from the client is correct, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server. *("the server verifies the validity of auth_token. If it is valid, the server sends a message to the client giving him permission to access the server" pg. 4)*

Peyvarian does not explicitly teach the server responds to the client by generating a one-time challenge token that depends at least on a first random value and sending the challenge token to the client;

The ATIS Committee defines a message authentication code (MAC) as "A bit string that is a function of both data (either plaintext or ciphertext) and a secret key, and that is attached to the data in order to allow data authentication."

It would have been obvious to one of ordinary skill in the art at the time of the invention to use a MAC as a challenge token, where the examiner interprets the challenge token as data encrypted with a secret key.

The motivation to use a MAC is for "allowing a receiver to verify the integrity of the message" (ATIS definition).

Office Action dated March 29, 2007, pages 4-5.

Claim 1, which is representative of the other rejected independent claims 9 and 17 with regard to similarly recited subject matter, reads as follows:

1. A computer network, comprising:

a client and a server connected by a network connection, wherein the client has a userid and a password associated with the client;

wherein the client requests access to the server by sending a first set of values to the server, wherein the first set of values includes a client-generated random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one;

wherein the server responds to the client by generating a one-time challenge token that depends at least on a server-generated random value and sending the challenge token to the client, wherein the server generates the challenge token by exclusive-oring the server-generated random value with a first hash, and wherein the first hash is a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client-generated random value;

wherein the client retrieves the server-generated random value from the challenge token and sends the server-generated random value and the userid to the server;

wherein the server verifies the received server-generated random value from the client is correct by comparing the server-generated random value received from the client with the server's stored value of the server-generated random number, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server;

wherein the client verifies the validity of the one-time authentication token received from the server;

wherein if the client verifies that the one-time authentication token from the server is valid, the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the result, the userid, and the message authentication code to the server;

wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code; and

wherein if the received message authentication code is verified, the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). For an invention to be *prima facie* obvious, the prior art must teach or suggest all claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

As amended, *Peyravian* and *ATIS*, taken alone or in combination, do not teach or suggest that "the client requests access to the server by sending a first set of values to the server, wherein the first set of values includes a client-generated random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one; wherein the server responds to the client by generating a one-time challenge token that depends at least on a server-generated random value and sending the challenge token to the client, wherein the server generates the challenge token by exclusive-oring the server-generated random value with a first hash, and wherein the first hash is a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client-generated random value; wherein the client retrieves the server-generated random value from the challenge token and sends the server-generated random value and the userid to the server; wherein the server verifies the received server-generated random value from the client is correct by comparing the server-generated random value received from the client with the server's stored value of the server-generated random number, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server, wherein the client verifies the validity of the one-time authentication token received from the server," as recited in independent claims 1, 9, and 17. In addition, *Peyravian* and *ATIS*, taken alone, do not teach or suggest that "if the client verifies that the one-time authentication token from the server is valid, the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the

result, the userid, and the message authentication code to the server; wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code; and wherein if the received message authentication code is verified, the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password," as recited in independent claims 1, 9, and 17.

Peyravian is directed to methods for protecting password transmission. The presently claimed invention refers to the cited *Peyravian* reference on page 3, of the specification and states that the schemes, such as in the cited *Peyravian* reference, do not provide protection against the offline password-guessing attack (i.e. dictionary attack) and denial of service attack. The claims of the present invention provide an improved method that provides this protection. There are many differences between the method and features of amended claims 1, 9, and 17 and the cited *Peyravian* reference. *Peyravian* does not teach or suggest that "the client requests access to the server by sending a first set of values to the server, wherein the first set of values includes a client-generated random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one; wherein the server responds to the client by generating a one-time challenge token that depends at least on a server-generated random value and sending the challenge token to the client, wherein the server generates the challenge token by exclusive-oring the server-generated random value with a first hash, and wherein the first hash is a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client-generated random value; wherein the client retrieves the server-generated random value from the challenge token and sends the server-generated random value and the userid to the server; wherein the server verifies the received server-generated random value from the client is correct by comparing the server-generated random value received from the client with the server's stored value of the server-generated random number, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server, wherein the client verifies the validity of the one-time authentication token received from the server," as recited in independent claims 1, 9, and 17. In addition, *Peyravian* does not teach or suggest that "if the client verifies that the one-time authentication token from the server is valid, the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the result, the userid, and the message authentication code to the server; wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code; and wherein if the received message authentication code is verified, the server changes the client password by replacing a digest of at

least the old password with a digest of at least the new password," as recited in independent claims 1, 9, and 17.

ATIS is directed to a definition of Message Authentication Code (MAC). The Examiner refers to the following portion of *ATIS* in the rejection of independent claims 1, 9, and 17:

> **message authentication code (MAC): 1.** A bit string that is a function of both data (either plaintext or ciphertext) and a secret key, and that is attached to the data in order to allow data authentication. *Note:* The function used to generate the message authentication code must be a one-way function. [2382-pt.8] **2.** Data associated with an authenticated message allowing a receiver to verify the integrity of the message. [INFOSEC-99]

ATIS, page 1.

ATIS merely defines a message authentication code. In the claims of the present invention, a message authentication code is computed and sent to the server by the client, and then the message authentication code is verified by the server prior to changing the client password at the server by replacing a digest of at least the old password with a digest of at least the new password. A message authentication code is not equivalent to the one-time challenge token as suggested in the Office Action. The message authentication code and the one-time challenge token are two different, distinct items in the claims of the present invention. In addition, *ATIS* does not teach or suggest that "the client requests access to the server by sending a first set of values to the server, wherein the first set of values includes a client-generated random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one; wherein the server responds to the client by generating a one-time challenge token that depends at least on a server-generated random value and sending the challenge token to the client, wherein the server generates the challenge token by exclusive-oring the server-generated random value with a first hash, and wherein the first hash is a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client-generated random value; wherein the client retrieves the server-generated random value from the challenge token and sends the server-generated random value and the userid to the server; wherein the server verifies the received server-generated random value from the client is correct by comparing the server-generated random value received from the client with the server's stored value of the server-generated random number, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server, wherein the client verifies the validity of the one-time authentication token received from the server," as recited in independent claims 1, 9, and 17. In addition, *ATIS* does not teach or suggest that "if the client verifies that the one-time authentication token from the server is valid, the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the result, the userid, and the

message authentication code to the server; wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code; and wherein if the received message authentication code is verified, the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password," as recited in independent claims 1, 9, and 17.

As stated above, there are many differences between the method and features of amended claims 1, 9, and 17 and the cited *Peyravian* reference. The addition of *ATIS's* definition for a message authentication code does not provide for the deficiencies of *Peyravian*. Thus, *Peyravian* and *ATIS*, taken individually or in combination, do not teach or suggest that "the client requests access to the server by sending a first set of values to the server, wherein the first set of values includes a client-generated random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one; wherein the server responds to the client by generating a one-time challenge token that depends at least on a server-generated random value and sending the challenge token to the client, wherein the server generates the challenge token by exclusive-oring the server-generated random value with a first hash, and wherein the first hash is a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client-generated random value; wherein the client retrieves the server-generated random value from the challenge token and sends the server-generated random value and the userid to the server; wherein the server verifies the received server-generated random value from the client is correct by comparing the server-generated random value received from the client with the server's stored value of the server-generated random number, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server, wherein the client verifies the validity of the one-time authentication token received from the server," as recited in independent claims 1, 9, and 17. In addition, *Peyravian* and *ATIS*, taken alone, do not teach or suggest that "if the client verifies that the one-time authentication token from the server is valid, the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the result, the userid, and the message authentication code to the server; wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code; and wherein if the received message authentication code is verified, the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password," as recited in independent claims 1, 9, and 17. Dependent claims 2-3, 6-8, 10-11, 14-16, and 18-24 are canceled. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-3, 6-11, 14-19 and 22-24 under 35 U.S.C. § 103(a).

III. 35 U.S.C. § 103, Obviousness

The Examiner has rejected claims 4, 12, and 20 under 35 U.S.C. § 103(a) as being unpatentable over *Peyravian* in view of *ATIS* as applied to claim 1 above, and further in view of *Searchsecurity.com*, www.searchsecurity.com, definition of one-time pad. This rejection is respectfully traversed.

Claims 4, 12, and 20 are canceled. Therefore, the rejection of claims 4, 12 and 20 under 35 U.S.C. § 103(a) has been overcome.

In addition, *Searchsecurity.com* does not provide for the deficiencies of *Peyravian* and *ATIS* with regard to independent claims 1, 9, and 17. *Searchsecurity.com* is directed to a definition of one-time pad. *Searchsecurity.com* does not teach or suggest that "the client requests access to the server by sending a first set of values to the server, wherein the first set of values includes a client-generated random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one; wherein the server responds to the client by generating a one-time challenge token that depends at least on a server-generated random value and sending the challenge token to the client, wherein the server generates the challenge token by exclusive-oring the server-generated random value with a first hash, and wherein the first hash is a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client-generated random value; wherein the client retrieves the server-generated random value from the challenge token and sends the server-generated random value and the userid to the server; wherein the server verifies the received server-generated random value from the client is correct by comparing the server-generated random value received from the client with the server's stored value of the server-generated random number, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server, wherein the client verifies the validity of the one-time authentication token received from the server," as recited in independent claims 1, 9, and 17. In addition, *Searchsecurity.com* does not teach or suggest that "if the client verifies that the one-time authentication token from the server is valid, the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the result, the userid, and the message authentication code to the server; wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code; and wherein if the received message authentication code is verified, the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password," as recited in independent claims 1, 9, and 17. Thus, any alleged combination of *Peyravian*, *ATIS*, and *Searchsecurity.com* still would not result in the invention recited in claims 1, 9, and 17.

IV. 35 U.S.C. § 103, Obviousness

The Examiner has rejected claims 5, 13, and 21 under 35 U.S.C. § 103(a) as being unpatentable over *Peyravian* in view of *ATIS*, further in view of *Searchsecurity.com* as applied to claim 4 above, and further in view of *Jablon* (U.S. Patent No. 6,792,533). This rejection is respectfully traversed.

Claims 5, 13, and 21 are canceled. Therefore, the rejection of claims 5, 13 and 21 under 35 U.S.C. § 103(a) has been overcome.

In addition, *Jablon* does not provide for the deficiencies of *Peyravian*, *ATIS*, and *Searchsecurity.com* with regard to independent claims 1, 9, and 17. *Jablon* is directed to a method for two parties to use a small shared secret to mutually authenticate one another over an insecure network. *Jablon* does not teach or suggest that "the client requests access to the server by sending a first set of values to the server, wherein the first set of values includes a client-generated random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one; wherein the server responds to the client by generating a one-time challenge token that depends at least on a server-generated random value and sending the challenge token to the client, wherein the server generates the challenge token by exclusive-oring the server-generated random value with a first hash, and wherein the first hash is a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client-generated random value; wherein the client retrieves the server-generated random value from the challenge token and sends the server-generated random value and the userid to the server; wherein the server verifies the received server-generated random value from the client is correct by comparing the server-generated random value received from the client with the server's stored value of the server-generated random number, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server, wherein the client verifies the validity of the one-time authentication token received from the server," as recited in independent claims 1, 9, and 17. In addition, *Jablon* does not teach or suggest that "if the client verifies that the one-time authentication token from the server is valid, the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the result, the userid, and the message authentication code to the server; wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code; and wherein if the received message authentication code is verified, the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password," as recited in independent claims 1, 9, and 17. Thus, any alleged combination of *Peyravian*, *ATIS*, *Searchsecurity.com*, and *Jablon* still would not result in the invention recited in claims 1, 9, and 17.

V. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: June 14, 2007

Respectfully submitted,

/Gerald H. Glanzman/
Gerald H. Glanzman
Reg. No. 25,035
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants

GHG/VJA